

AN EFFICIENT SECURITY PROTOCOL FOR ADVANCED METERING INFRASTRUCTURE IN SMART GRID

Ye Yan, University of Nebraska-Lincoln

Rose Qingyang Hu, Utah State University

Sajal K. Das, The University of Texas at Arlington

Hamid Sharif, University of Nebraska-Lincoln

Yi Qian, University of Nebraska-Lincoln

ABSTRACT

In this paper, we present a security protocol for Advanced Metering Infrastructure (AMI) in smart grid. We consider various security vulnerabilities of deploying AMI, and explore the issues related to confidentiality for user privacy and behavior as well as message authentication for meter reading and control messages. After surveying the existing security solutions in this area, we propose a new protocol, called an integrated authentication and confidentiality (IAC) protocol, to provide efficient secure AMI communications in smart grid. With the help of the IAC protocol, an AMI system can provide trust services, data privacy and integrity by mutual authentications whenever a new smart meter initiates and joins the smart grid AMI network. Data integrity and confidentiality are fulfilled through message authentication and encryption services, respectively, using the corresponding keys established in mutual authentications. Simulation and analytical results show that the proposed IAC protocol has better performance in terms of end-to-end delay and packet loss when compared with a basic security scheme. Additionally, it can also facilitate efficient secure data collection and control message delivery between smart meters and a local collector for AMI communications in a smart grid.

Index Terms

Advanced metering infrastructure (AMI), smart grid, security, authentication, confidentiality, privacy, integrity

I. INTRODUCTION

Electrical power industry is in the process to integrate its distribution system with communication networks and control techniques to form a bi-directional power and information flow infrastructure, commonly called a smart grid. Such integration not only moves power automation systems from outdated technology to today's new communication technologies and systems, but also brings the proprietary network of power control systems to the public data networks. Although the integration results in greater performance benefit to the power industry, yet it leads to arduous challenges of protecting the smart grid system from vulnerability and security threats. As indicated in the Electric Power Research Institute (EPRI) report [1], cyber security is an extremely critical issue in smart grid due to increased potential of cyber-attacks and incidents against this critical sector of power grid as it becomes more and more interconnected. Cyber security must address deliberate attacks, such as those from disgruntled employees, industrial espionage, and terrorists, as well as inadvertent compromises of the information infrastructure due to user errors, equipment failures, and natural disasters. Vulnerabilities imply an attacker will have an opportunity to penetrate into a smart grid network, gain access to control software, and alter load conditions to destabilize the grid in unpredictable ways.

Various types of attacks targeting Industrial Control Systems (ICS) and Information Technology Systems (ITS) as well as different performance requirements of these traditional information systems determine a specific priority order of the security services implemented for smart grid communication systems. Threat profiles of the power transmission and distribution management functions, where availability is paramount to all other security services, differ significantly from threat profiles of ITS functions such as utility customer billing where confidentiality is a greater concern hence warranting different security concerns [2].

Advanced Metering Infrastructure (AMI) refers to systems that collect, measure, and analyze energy usage, from networks that are connected to the next-generation electricity meters, or so called smart meters. An AMI includes software, hardware, communication networks, customer-associated systems and meter data management system (MDMS). As smart grid becomes a reality, security threats are also expected to grow tremendously, from both inside and outside of the system. Utilities will almost certainly face substantial liability claims and regulatory fines if inadequate security technologies allow eavesdroppers, adversaries or hackers to acquire and use AMI data to a customer's detriment, or even worse, to interrupt services or hold utility customers as "hostage". Furthermore, if customers believe a utility is abusing personal identifiable data, or collecting information beyond what they deem acceptable, they are likely to resist the implementation of AMI. Since consumers may refuse to consent or hide their data, confidentiality of user privacy and behavior as well as authentication for meter reading and control messages are among two major security services that must be provided before an AMI can be widely deployed in smart grid.

In the literature, there exists limited research on AMI authentication and confidentiality of user data privacy and behavior [3-9]. In this paper, we present an efficient, integrated authentication and confidentiality (IAC) protocol for secure AMI communications in smart grid. First, we develop a mutual authentication procedure that establishes secure key pairs between authentication server and smart meters for AMI communications. Next, a collaborative data aggregation and forwarding scheme is provided between smart meters and a local data collector/distribution point to fulfill efficient and secure

communications for meter-reading collecting and management message dispatching. We evaluate the performance of the proposed IAC protocol through simulation experiments and security analysis. Experimental results show that the IAC protocol can provide efficient and secure AMI communications with acceptable end-to-end delay and packet loss.

The rest of this paper is organized as follows. Section II provides a brief description of smart grid AMI communication network architecture and its cyber security requirements, followed by a review on the existing AMI security solutions. Section III proposes the IAC protocol while Section IV presents its performance evaluation and security analysis. Section V summarizes the paper with directions of future work.

II. BACKGROUND

This section provides an overview of a smart grid AMI communication network architecture, on which our proposed security protocol will be based on. It also describes security requirements for AMI communications, followed by a literature review on the existing security solutions related to it.

SMART GRID AMI COMMUNICATION ARCHITECTURE

AMI is one of the critical parts of a smart grid system. Its key requirement is to ferry the metering data from the customer premises to the Meter Data Management System (MDMS) of the utility provider. The range of communication technologies is wide, a diverse mix of public and private, wired and wireless, standard and proprietary technologies [10, 11].

Figure 1 depicts a generic communication network architecture for smart grid AMI, which is generalized from the literature [4, 11]. Typically, the network topology consists of several trees, each rooted at the feeder, such that the meter nodes in a locality send metering data over wireless links (via multiple hops, if necessary) to a nearby feeder. The feeder in turn sends data over a wide area network connection to the MDMS local management office. Specifically, the Supervisory Control and Data Acquisition (SCADA) systems have been implemented to monitor and control electrical power grids for decades [11]. The central SCADA manages the electricity supply to substations on high voltage (> 230 KV) transmission lines. Usually, the handoff from high voltage electricity transmission to middle voltage (11 KV) electricity distribution for feeder lines takes place in substations. After the voltage transformation at the end of the feeder line, a consumer terminal gets low voltage (110 V/220 V) electricity at home. At each home, smart meters collect electricity power consumption data online from all intelligent appliances and send them back to a local management office of the utility company. Those data are first processed as billing information, then aggregated and further forwarded to the SCADA system. With the help of real-time power consumption information from terminal consumers, the utility operator can monitor and diagnose on-line the status of the entire smart grid system, and optimally adjust the power generation, transmission and distribution. It can smooth peak demand and avoid potential blackout at the utility side. Real-time management messages are distributed to the corresponding consumers backward to smart meters through the AMI system. Therefore, intelligent appliances accordingly re-schedule their tasks to avoid power demand rush hours as well as to reduce blackout possibility at the consumer side.

In the AMI network architecture in Figure 1, the communication infrastructure for low voltage electricity distribution network is usually implemented by wireless mesh networking technologies for a group of terminal consumers. For simplicity, each terminal consumer is considered as a smart meter and the intelligent appliances in a home are covered by a smart meter.

In other words, a smart meter is a home portal for AMI communications in the smart grid. These smart meters are connected to a feeder line which acts as a gateway and forwards the collected meter-readings to the local management office using a wide area network connection. These meter-readings are recorded for individual customers and the aggregated readings are further forwarded to the central SCADA for system monitoring, demand management and operation optimization.

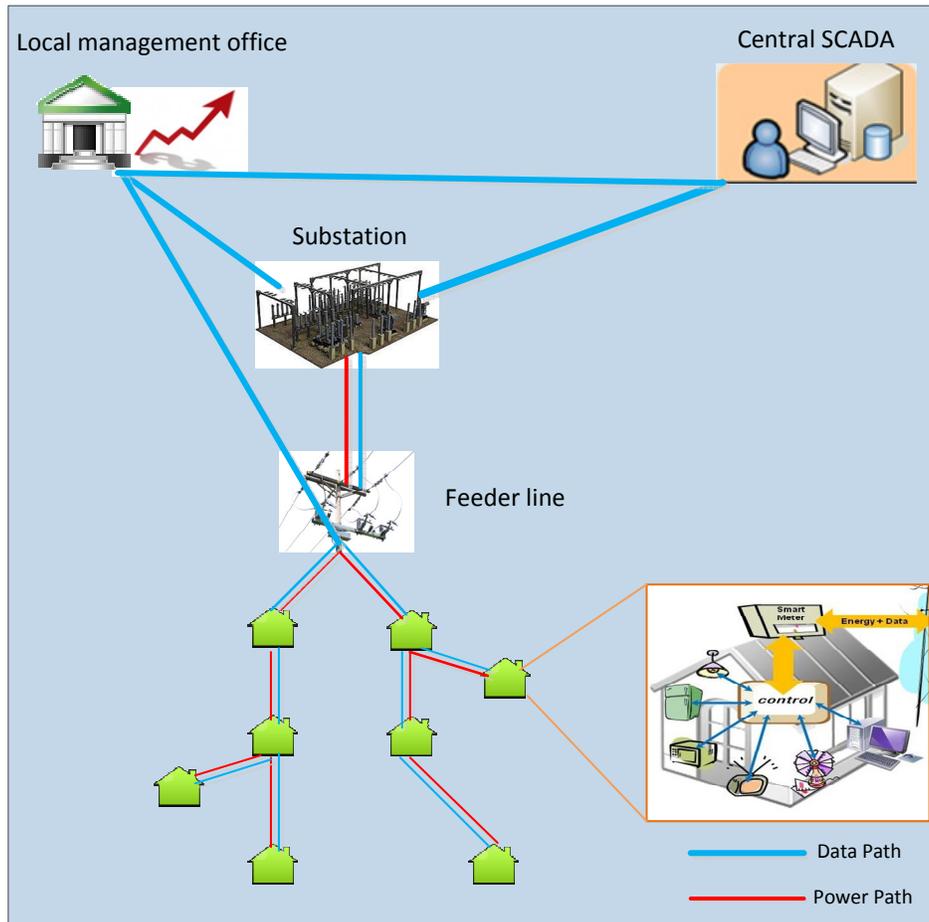


Figure 1 A smart grid AMI communication network architecture

AMI SECURITY REQUIREMENTS

When initially entering the AMI network, each smart meter must be verified as a legal device and terminal customer by the remote authentication server located at the local management office. Unique security mechanisms are needed to ensure the integration, availability and privacy of both meter-reading data and management messages. In such security mechanisms, the cryptographic overhead including digital certificates and signatures is quite significant for an embedded device like smart meter in smart grid AMI compared to normal personal computers in regular enterprise network. Additionally, cryptographic operations contribute significantly to the computational cost, especially at the recipient end, which verifies the message. In a smart grid system, a smart meter typically sends each meter-reading message in an interval of several seconds to a few minutes. A digital signature in such a time interval can be generated by a Public Key Infrastructure (PKI). However, for smart grid system that connects hundreds of buildings, each with possibly a large number of apartments, the number of

meter-reading messages to be verified might be overwhelming its capacity. In addition, the adoption of wireless and IP technologies exposes smart grid AMI communications to the traditional cyber attacks such as resource depletion attack, masquerade attack, etc. [10].

Although digitally signing and verifying each message can enhance security of communications, schemes based on conventional cryptographic operations are neither efficient nor scalable to the traffic density and resource constraints in a smart grid system. We need light-weight yet secure and efficient schemes tailored specifically for smart grid AMI communications so that the meter-reading data collection and management message distribution can be processed securely and efficiently.

To address the above cyber security threats, the general requirements for AMI security can be summarized as follows [6].

- *Device authentication*: The identity and legality of the smart meters and associated consumers should be verified before joining the interconnected smart meter network and receiving proper utility service.
- *Data confidentiality*: The smart meter readings and management control messages should be kept confidential to conceal consumer privacy and utility operator's business information from unauthorized entities.
- *Message integrity*: The smart grid should be able to ensure meter-reading or management messages to be delivered unaltered in AMI.
- *Maintaining secrecy*: Some parts of the secrecy of a smart meter should be kept in privacy while other parts may be shared with designated partners for secure communications.
- *Preventing potential cyber-attacks*: A smart meter, by holding own digital credential, should be guaranteed to obtain secure connections with the smart meter network. Even if an individual smart meter is attacked, the adversary should not leverage the compromised meter to access information on other meters or penetrate into the AMI of the smart grid.
- *Facilitating communication overhead*: Any proposed new secure AMI communication protocol should be efficient in terms of communication overhead and processing latency.

RELATED WORK

There exists some recent work addressing authentication and confidentiality of AMI communications in smart grid [3]. In [4], the authors proposed a new utility security management and authentication scheme for action/command requests in the host Area Electric Power System (AEPS) and interconnected multiple neighboring AEPS. Secure and intuitive device authentication techniques for the smart grid enabled Home Area Networks (HANs) are proposed in [5], where the authors assumed a distributed architecture for a HAN consisting of smart appliances, a smart meter and a gateway. In this architecture, the operating schedules of the appliances are controlled by the gateway based on pricing and control messages from smart meter. Three different device authentication mechanisms in the HAN demonstrated how to prevent adversarial behaviors during device authentication such as man-in-the-middle and impersonation attacks. Focusing on authentication protocols, in [6] the authors discussed the key design principles and engineering practices that can help ensure the correctness and effectiveness of authentication standards in power grid protocols. In contrast, user privacy and user behavior

confidentiality in smart grid communications has received only little attention. A method for secure anonymization of frequent electrical metering data was described in [7]. It provided a third party escrow mechanism for authenticated anonymous meter readings which are difficult to associate with a particular smart meter or customer. The privacy issues implicated by the development of demand response systems were explored in [8], which demonstrated that the data collected by AMI reveals detailed information about the user behavior within home. This work also showed how new system architectures based on privacy-aware design principles realize the benefits of demand response without requiring centrally collected AMI data. In [9] we introduced a secure and reliable collaborative communication scheme for AMI. To the best of our knowledge, none of the existing studies addressed the efficiency and scalability issues for authentication and privacy mechanisms between smart meters and management office in the AMI communication networks in smart grid. This motivates our work in this paper.

III. PROPOSED IAC PROTOCOL

In this section, we propose the Integrated Authentication and Confidentiality (IAC) protocol for efficient and secure AMI communications which can work with current industrial standards such as ANSI C12 protocol suite [12]. The proposed IAC protocol includes the following processes: (1) Initialization process for authentication; (2) Meter-reading collection process for user data confidentiality; (3) Control message distribution process for control message confidentiality. The IAC protocol is based on the communication network architecture in Figure 1 with a hop-by-hop data aggregation and forwarding scheme. Both efficiency and security can be achieved in our proposed IAC approach. It can cover the user data privacy and integration which is the unique and main concern in AMI security requirement by collaborative data aggregation along the data collecting path.

Initialization Process

Figure 2 illustrates the initialization process for each new smart meter as a supplicant. Before joining the AMI network, each new smart meter must be verified by the remote authentication server located at the local management office as a legal device and terminal customer. The neighboring authenticated smart meters can play as authenticators in the initialization process and relay the authentication process messages between the supplicant and the authentication server. Both the supplicant and the authentication server have an identical key K , which was pre-installed, not concealed to anyone else including the authenticator. Both the mutual authentication identities and the consequent data encryption/decryption between supplicant and authentication server are based on K . If the supplicant's identity is authenticated as a valid device, the corresponding credential of the supplicant is established between the authentication server and the supplicant. Then, the authentication server will generate an initial vector (IV) and a key k . The IV and k will be encrypted by K , denoted as $E_K(IV||k)$ as shown in Figure 2. So the supplicant can decrypt and get its IV and k . Meanwhile, the authentication server sends k to the authenticator encrypted with their own K' denoted as $E_{K'}(IV||k)$ since the authenticator was authenticated already with K' . So the authenticator knows k . With its k , the supplicant and authenticator can individually generate $k_{n-1,n}$, which is the symmetric key for message authentication code generation and validation between one-hop neighboring nodes n and $n - 1$ on the data forwarding path. As such, a four-way handshake procedure is established to fulfill another mutual authentication between the supplicant and authenticator. After successful mutual authentication, the key $k_{n-1,n}$ at both supplicant and authenticator sides is validated and made ready for subsequent message authentication code generation and validation purpose. After the

initialization process, the proposed IAC protocol also includes a hop-by-hop data aggregation and forwarding scheme that transmits meter-reading and control messages between smart meters and a feeder (collecting node), as described in the following.

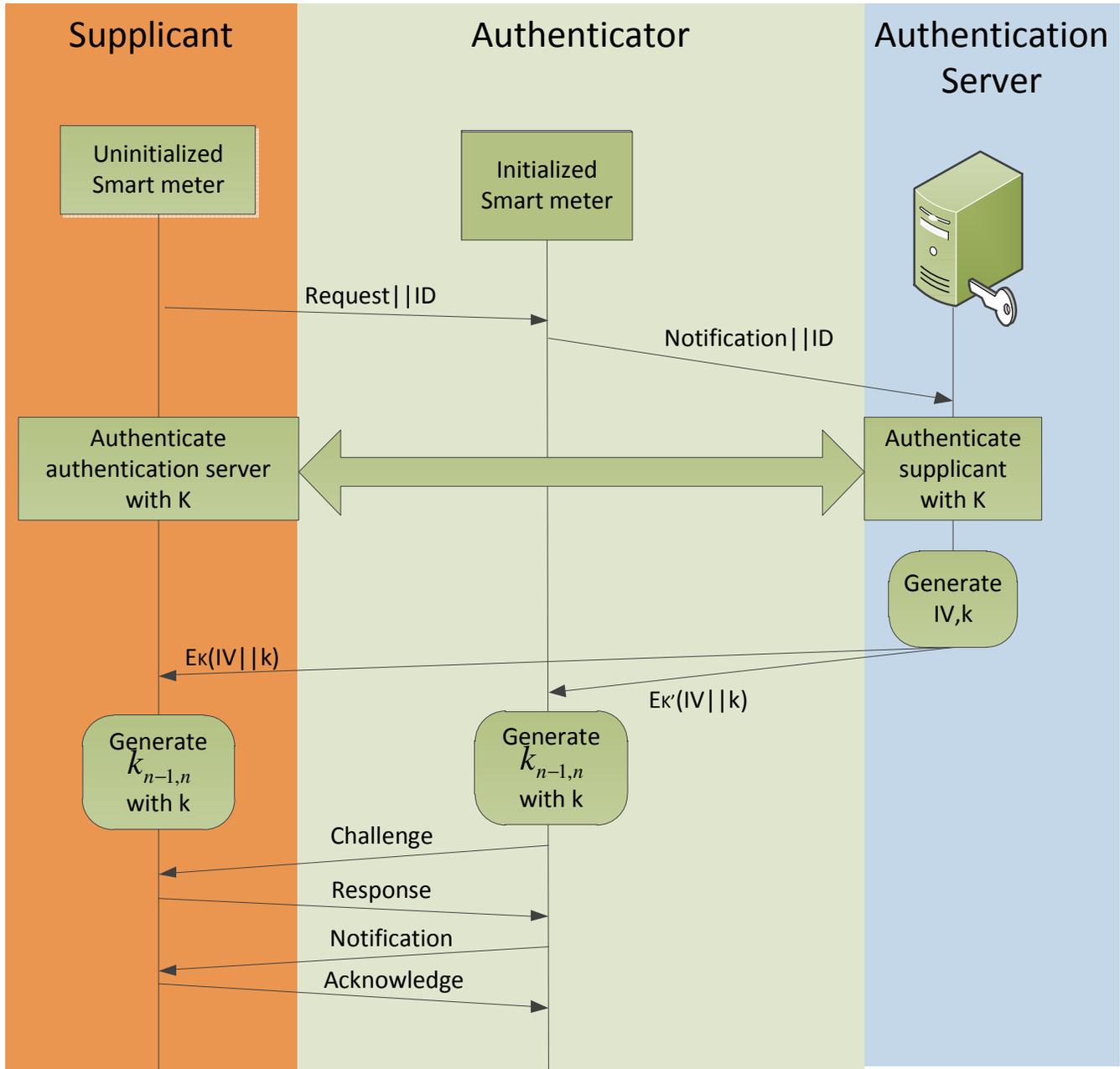


Figure 2 Initialization process and authentication

Hop-by-hop Data Aggregation and Forwarding

Since every smart meter must fulfill the initialization process before it enrolled in data communication, the back-end authentication server can collect all the necessary topology information of the multi-hop smart meter mesh network. The back-end server can generate the optimal routing backbone such as discussed in [13], and notify the corresponding smart

meters dynamically. In the rest of this paper, our proposed IAC protocol assumes that a group of smart meters form a chain topology through a wireless backbone in the order of node 1, node 2, ..., node n , and the collecting node at the end. The proposed security protocol performs encryption and message authentication tasks in N repeated operations (with different keys for each operation) from every source smart meter to the collecting node. These operations will be distributed to a subset of smart meter nodes on the wireless backbone. Compared to a basic end-to-end security scheme which performs the encryption and message authentication at the source/destination node only, this hop-by-hop data aggregation and forwarding approach can enhance the system security performance by grouping a certain intermediate nodes together with source/destination node. By using this approach, the efficiency and reliability of the multi-hop wireless network for AMI can be improved.

Algorithm_BNS is the backbone node selection (BNS) algorithm we propose to construct the backbone chain for IAC protocol when the data aggregation and forwarding route is needed. It is equivalent to a wireless mesh network of smart meters to a feeder in AMI as shown in Figure 1. The backbone node selection algorithm should be simple and efficient to select the backbone nodes and to construct or rebuild the backbone in a scalable way for AMI system in case router error occurred, especially time varying wireless channel errors. The selected intermediate backbone nodes work in a hop-by-hop mode. The corresponding keys K_n (the K of node n) and $k_{n-1,n}$ can be piggybacked in the backward routing messages during the initialization process. Those selected intermediate nodes without encryption and authentication process are simply relaying the packets. We only focus on the selected intermediate nodes with encryption and authentication process.

Algorithm_BNS (Backbone Node Selection)

```

1: Input: The total number of nodes on the routing path of wireless backbone  $s$ , the length (hop count) of the routing path  $n - 1$ , the number of intermediate backbone nodes that the BNS algorithm should choose  $N$ , the set of nodes on the routing path of the wireless backbone  $V = v_1, v_2, \dots, v_{(n-1)}$ , and the set of loads to nodes on the routing path  $L = L_1, L_2, \dots, L_{(n-1)}$ 
2: Output: the set of selected backbone node (BNs)  $S \subseteq \{v_1, v_2, \dots, v_{(n-1)}\}$ 
3: Initialization:  $S := \emptyset; s = 0; Rand := \emptyset$ 
4: for  $i = 1$  to  $N$  do
5:   for  $j = 1$  to  $n$  do
6:     if  $v_j \in S$  then
7:        $j = j + 1$ 
8:     end if
9:     if  $L_j \leq s$  then
10:       $s = L_j; index = j; Rand = Rand + v_j$ 
11:    end if
12:     $j = j + 1$ 
13:  end for
14:  $S = S + \text{random}(Rand); i = i + 1;$ 
15: end for
16: RETURN  $S$ 

```

Meter-reading Collection Process

Figure 3 illustrates the encryption/decryption and authentication process for meter-reading collection. The smart meter node 1 at the beginning of a routing chain conducts an XOR (+) operation using its plaintext meter-reading message with its own

initial vector IV . The result is then used to generate the encrypted message M_1 by using key K_1 . The message authentication operation uses M_1 and $k_{1,2}$ to generate the corresponding message authentication code which will be appended to M_1 . Both M_1 and the corresponding message authentication code (C) are sent to its neighboring smart meter node 2 next to the collecting node. Smart meter node 2 generates its own message authentication code with $k_{1,2}$ and the received M_1 . If the generated code matches the received one, the integrity of M_1 is verified. Afterwards, M_1 runs as the input to XOR operation with reading of smart meter node 2. A similar process takes place in all the intermediate nodes in the routing chain until it reaches the collecting node, which has K_n 's of all the nodes along the route. After the message authentication is validated with the smart meter node n , the collecting node can decrypt all the readings from smart meters 1 to n along the routing chain at once.

The collecting node aggregates the received meter-readings and forwards the processed data via dedicated lines or an overlay network to its upstream. All meter-readings on the feeder lines are collected in the local management office, where real-time readings are reordered for billing purpose. The information extracted from the real-time meter-readings is utilized not only by local management office and/or substation, but also by the central SCADA system operation.

Control Message Distribution Process

Since the remote central SCADA and local management office/substation will adjust the power generation, transmission and distribution in the smart grid according to the collected meter-readings, the management and control messages will be distributed to specific smart meters to schedule intelligent home appliance operations. Figure 4 shows the reverse process flow as compared to Figure 3, which can be used to cast specific management messages from the collecting node to the specific smart meter nodes on the routing chain. Note that in the proposed IAC protocol, both authentication and encryption processes are performed hop-by-hop along the communication route.

IV. PERFORMANCE EVALUATION AND SECURITY ANALYSIS

Simulation Setting

We evaluate the system performance of our proposed IAC protocol by using ns-2 simulation and security analysis. In the simulation studies, the data collecting node is modeled as a PC processor while a smart meter node is modeled as an ARM processor. IEEE 802.11b standard are adopted as the underlying wireless PHY/MAC protocol. We compare the performance of the proposed IAC protocol with that of a basic security scheme, where each smart meter communicates with the collecting node through a private key and an end-to-end encryption through the same multi-hop routing chain of the IAC protocol, in which we call it "basic security scheme" or simply "basic scheme". End-to-end delay is crucial for real time applications such as online meter-readings collection for electricity voltage, current, phase and reactive power status in the smart grid. If the data cannot meet its end-to-end deadline, it might cause serious system fault especially in the monitoring/protecting system for missing the fault detection. Packet drop rate is also important for the system to make prompt and proper decision based on the collected real-time meter readings.

A node's transmit power set to the minimum value ensures sufficient coverage only between two immediate nodes so that there is very little interference to other nodes on the data collection/distribution path. The metering data traffic is generated as a Constant-Bit-Rate (CBR) type UDP session at rate 1 packet/second with packet size of 50 bytes for each meter node. The destination of hop by hop path is the data collecting node. Following [14], in each smart meter and the back-end collecting

node, we use a block cipher SEED for encryption/decryption, with each data block taking 19.23 μs processing time on ARM processor and 3.4 μs processing time on PC processor. We use Hash-based Message Authentication Code (HMAC) for message authentication code generation, with each data block taking 23.63 μs processing time on ARM processor and 3.68 μs processing time on PC processor.

Experimental Results

Figures 5(a) and 5(b) respectively show the average end-to-end packet delay and average packet delivery rate for the proposed IAC protocol and the basic scheme, as a function of the total number of hops in the routing chain. When the number of hops increases, the end-to-end packet delay increases and the packet delivery rate decreases for both security schemes. However, the performance of our IAC protocol is consistently better than the basic security scheme for both metrics.

Figures 5(c) and 5(d) further show end-to-end packet delay and packet delivery rate collected from each of the smart meter node along a particular route with 9 hops. Meter 1 is the closest while Meter 9 is the furthest from the collection node. From Figure 5(c), the packets generated at the nodes that are less than 5 hops away from the collection/destination node experience a smaller end-to-end packet delay if a basic security scheme is used. On the other hand, those packets experience a smaller end-to-end packet delay if the IAC scheme is used. The packet delay collected from different nodes belonging to the same routing chain is the same in the IAC scheme, which can be explained as follows. In the IAC protocol, the packets from different nodes are generated synchronously and combined into a super data packet using the proposed *hop-by-hop data aggregation and forwarding scheme*. The super packet is then received and decoded by the collection node all together. From Figure 5(d) we observe that, the further a smart meter, the worse is its packet delivery rate. The packet delivery rate at each smart meter is always higher if the IAC scheme is used. The nature of 802.11b is contention based. The packet collision rate at each node could be high as the number of wireless devices goes up. The proposed IAC protocol can arrange the transmission schedule for each participating smart meter at the initialization process. Therefore, all the participating smart meters transmit in a pre-defined order to reduce collision.

Security Analysis

In cryptography, security is typically measured in the context of uncertainty – the property of hiding the information in a message. Typically, security levels are analyzed stochastically in probabilities and/or distributions. However, it is useful to quantify the security levels using information theoretic metrics such as entropy. The strong security property should be guaranteed to hide user privacy related information, especially for the smart meter reading data in AMI networks. The nature of information security evaluation problem allows us to use a stochastic quantity called relative entropy [15], a well-known information theoretic metric, to evaluate the relative uncertainty to information. To evaluate this metric in the proposed IAC protocol, we assume that the proposed IAC protocol and the basic scheme are modeled as stochastic processes with probability mass function p_i and q_i , respectively. For data aggregation on the path, there are $m = \lceil L/M \rceil$ possible trials to determine the right data partition M_i ($i = 1, \dots, m$), where L is the entire data payload length and M is the data block size. If an attacker has no knowledge on the network topology and uses a brute force search, according to the log sum inequality [15], the lower bound of the relative entropy can be expressed as

$$\sum_{i=1}^{mM} (p_i \log \frac{p_i}{q_i}) \geq \left(\sum_{i=1}^{mM} p_i \right) \log \frac{\sum_{i=1}^{mM} p_i}{\sum_{i=1}^{mM} q_i}$$

The comparison of the system security can be measured through relative entropy of the IAC protocol to the basic scheme. As illustrated in Figure 5(e), the relative entropy increases as the total number of hops in the routing chain increases, which means more uncertainty is introduced in the IAC protocol than the basic scheme. This translates to stronger security for the proposed IAC protocol; the higher the relative entropy, the stronger is the system security.

We define *efficiency ratio* of a security scheme as the ratio of the number of security overhead bits to the number of data payload bits. Figure 5(f) shows the efficiency ratio of the proposed IAC protocol for two HMAC schemes with 128 bits and 160 bits, respectively. We can see that HMAC-128 has better efficiency ratio than HMAC-160 due to its lower overhead. We also observe that as the number of hops in the routing chain increases, the efficiency ratio goes up.

The above performance results demonstrate that when the number of hops in the routing chain increases, the two security metrics – relative entropy and efficiency ratio – are also improved while the two QoS metrics – end-to-end delay and packet delivery ratio – are deteriorated. Therefore, careful tradeoff must be made to achieve the desirable performance when deploying the smart grid AMI network.

V. CONCLUSIONS

As a critical part of the smart grid communication infrastructure, AMI will face a variety of cyber security threats that impair the reliability and efficiency of smart grid operations. In this paper, we investigated unique cyber security concerns in smart grid AMI system, and proposed a secure and efficient IAC protocol for meter data collecting and management message distribution in AMI communications. The proposed IAC protocol employs mutual authentication between a remote server located in the local management office and a neighboring smart meter as the authenticator to obtain proper cryptography keys for consequent secure data communications. Therefore, readings from smart meters and management messages from central SCADA and/or local management office can employ encryption and message authentication mechanisms tailored for the security requirements and the system constraints. Simulation results show that the proposed IAC protocol has lower end-to-end delay as well as lower packet loss. Security analysis show that our proposed IAC protocol can provide more secure and efficient data collection and management message delivery between smart meters and a local collector. The future work will first focus on how to adapt the proposed IAC protocol to multicast and broadcast in smart grid AMI networks. The second direction of the future work will investigate the impact of error prone wireless channel on the proposed IAC protocol, and the possible improvement of the IAC protocol under the error prone wireless channel.

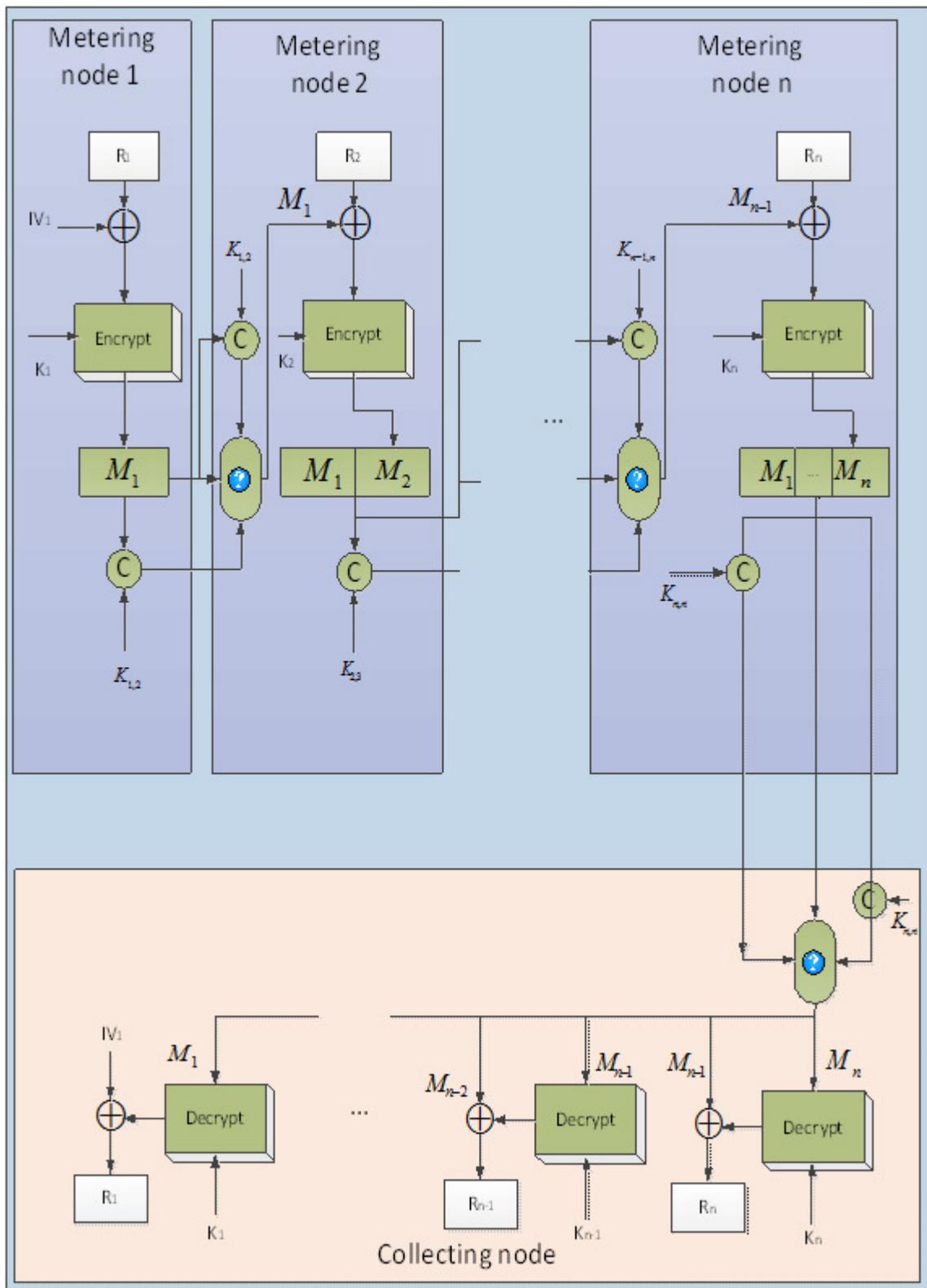


Figure 3 Meter-reading collection process

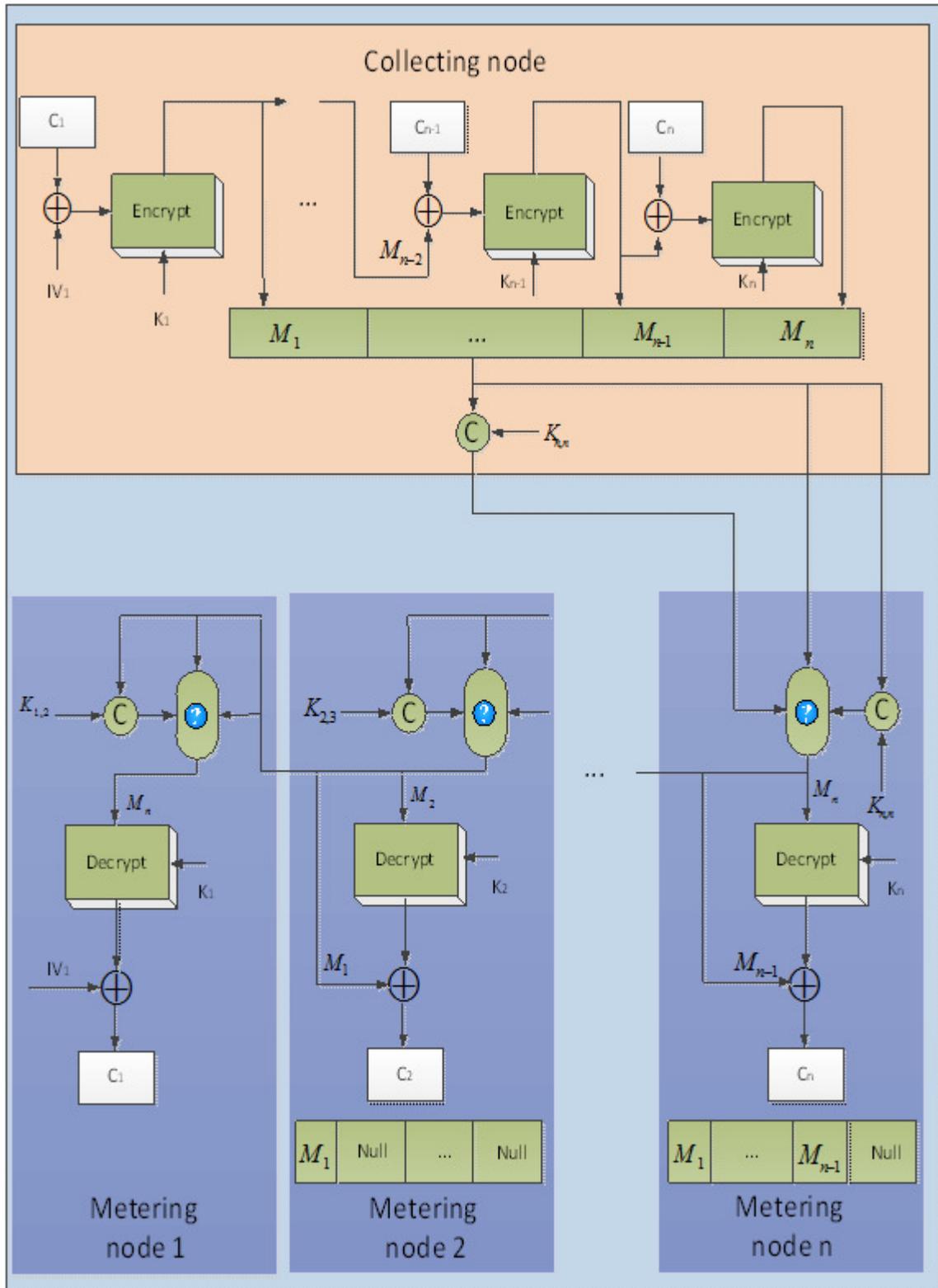


Figure 4 Control message distribution process

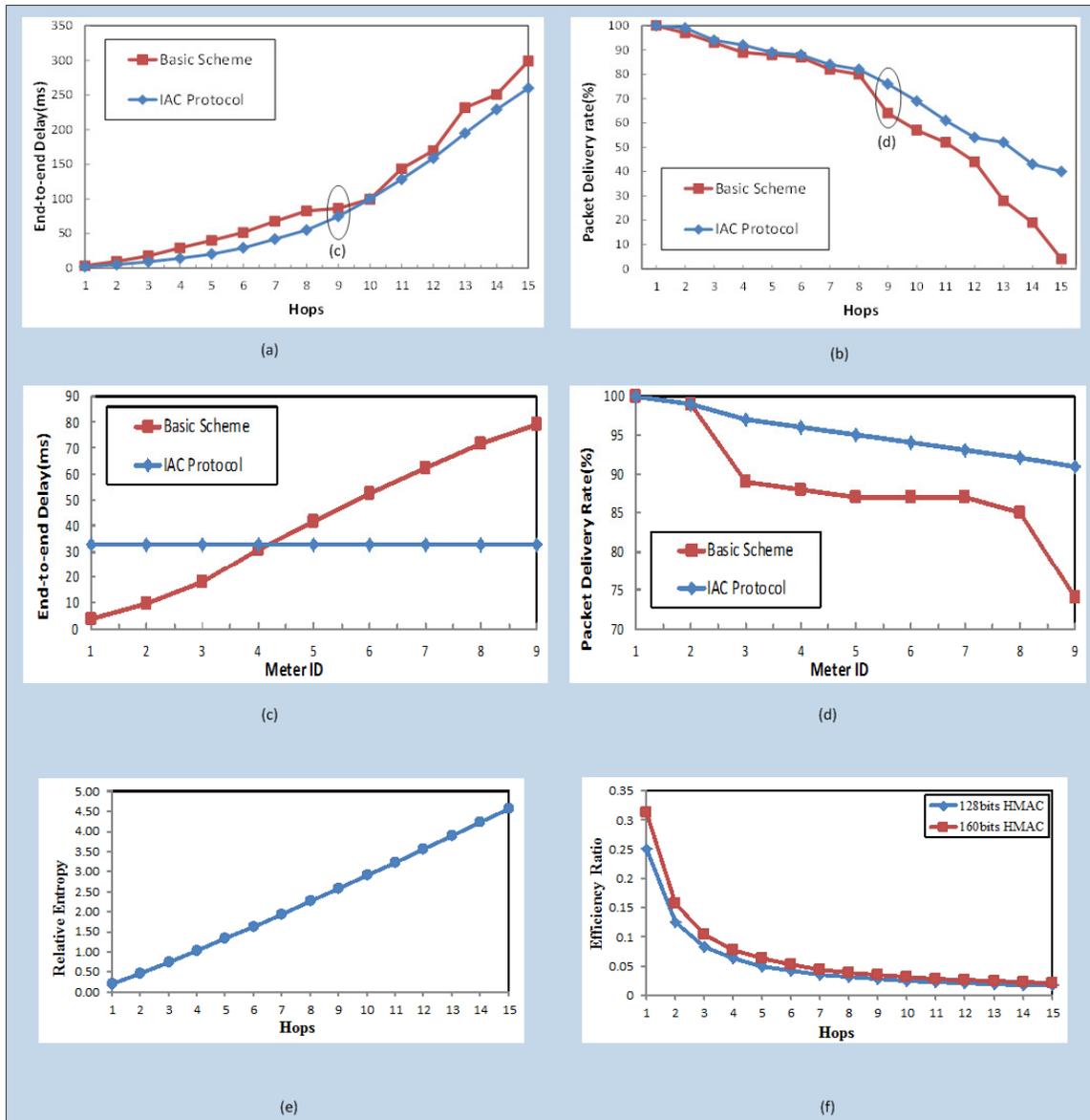


Figure 5 Performance comparison and security analysis of the proposed IAC protocol and a basic scheme

REFERENCES

- [1] Electric Power Research Institute, "Report to NIST on smart grid interoperability standards roadmap," 2009.
- [2] P. D. Ray, R. Harnoor, and M. Hentea, "Smart power grid security: A unified risk management approach," IEEE International Carnahan Conference on Security Technology (ICCST2010), 5-8 Oct., 2010.
- [3] Z. Fan, P. Kulkarni, S. Gormus, C. Efthymiou, G. Kalogridis, M. Sooriyabandara, Z. Zhu, S. Lambotharan, and W. Chin, "Smart Grid Communications: Overview of Research Challenges, Solutions, and Standardization Activities," IEEE Communications Surveys & Tutorials, pp. (99):1-18. 2012

- [4] A. Hamlyn, H. Cheung, T. Mander, L. Wang, C. Yang, and R. Cheung, "Computer network security management and authentication of smart grids operations," in IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, pp. 1-7, 2008.
- [5] E. Ayday and S. Rajagopal, "Secure, intuitive and low-cost device authentication for Smart Grid networks," in IEEE Consumer Communications and Networking Conference (CCNC 2011), pp. 1161-1165, 2011.
- [6] H. Khurana, R. Bobba, T. Yardley, P. Agarwal, and E. Heine, "Design principles for power grid cyber-infrastructure authentication protocols," in 43rd Hawaii International Conference on System Sciences (HICSS 2010), pp. 1-10, 2010.
- [7] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in First IEEE International Conference on Smart Grid Communications (SmartGridComm 2010), pp. 238-243, 2010.
- [8] S. Wicker and R. Thomas, "A privacy-aware architecture for demand response systems," in 44th Hawaii International Conference on System Sciences (HICSS 2011), pp. 1-9, 2011.
- [9] Y. Yan, Y. Qian, and H. Sharif, "A secure and reliable in-network collaborative communication scheme for advanced metering infrastructure in smart grid", Proceedings of IEEE WCNC 2011, March 2011.
- [10] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A Survey on Cyber Security for Smart Grid Communications," IEEE Communications Surveys & Tutorials, pp(99):1-13. 2012.
- [11] G. A. Taylor, M. R. Irving, P. R. Hobson, C. Huang, P. Kyberd, and R. J. Taylor, "Distributed monitoring and control of future power systems via grid computing," in IEEE Power Engineering Society General Meeting, 2006.
- [12] A. F. Snyder and M. T. G. Stuber, "The ANSI C12 protocol suite - updated and now with network capabilities," in Power Systems Conference: Advanced Metering, Protection, Control, Communication, and Distributed Resources, 2007. PSC 2007, 2007, pp. 117-122.
- [13] H. Guo, Y. Qian, K. Lu and N. Moayeri, "Backbone construction for heterogeneous wireless ad hoc networks," in IEEE International Conference on Communications, 2009 (ICC'09), pp.1-5, June 2009.
- [14] S. Hong, M. Lee, D. Shin, "Experiments for embedded protection device for secure SCADA communication," in Asia-Pacific Power and Energy Engineering Conference (APPEEC 2010), pp.1-4, March 2010.
- [15] T. M. Cover and J. A. Thomas, *Elements of information theory*, John Wiley & Sons, Inc. New York, NY, USA, 2006.